

REMARKS

Claims 26 - 32 have been added. Claims 1-32 are pending in the application.

I. Rejection of claim 23 under 35 U.S.C. 112

The examiner has rejected claim 23 under 35 U.S.C. 112. The applicant respectfully traverses this rejection. The examiner states that:

"The specification does not explain how a portable device is a PCMCIA card or the specification does not explain how the first device is a PCMCIA port." (4/6/2005 office action, pg. 2, last paragraph).

The examiner is incorrect. The specification specifically refers to a device 720, which is portable, which may be a PCMCIA card, which is further defined as a "personal computer modem computer input access" card. (Present application, Figs. 11A, 11B, pg. 14). The specification also clearly refers to a device 730 which may be a PCMCIA port. (Id.).

Claim 23 is submitted to be allowable.

II. Rejection of claims 1-3, 14-17, 19-21 and 25 under 35 U.S.C. 103(a) based on Southerland in view of Varadharajan

The examiner has rejected claims 1-3, 14-17, 19-21 and 25 under 35 U.S.C. 103(a) based on Southerland in view of Varadharajan. These rejections are respectfully traversed.

Claim 1 specifies as follows:

1. A method comprising:
 - placing a first device in an enclosure;
 - placing a second device in the enclosure;
 - sealing the enclosure while the first device and the second device are in the enclosure;
 - causing the first device to exchange a key with the second device while the first device and the second device are in the enclosure and while the enclosure is sealed;
 - removing the first device and the second device from the enclosure after the key exchange; and
 - using the key to allow the first device and the second device to communicate with each

other using methods of encryption outside the enclosure.

In the present application, in one or more embodiments, a first device 100 and a second device 200 are placed in an enclosure 10. (Present application, pg. 9-10, Fig. 1). The enclosure 10 is sealed. (Id.) The first device 100 exchanges a key with the second device 200 while the first device 100 and the second device 200 are in the enclosure 10 and while the enclosure 10 is sealed. (Id.) The first device 100 and the second devices 200 are removed from the enclosure 10 after the key exchange and thereafter the two devices communicate with each other with the key using methods of encryption outside of the enclosure 10. (Id.)

Southerland discloses active erasure of data in a volatile data storage device when a tamperer intrudes into a "secure environment". (Southerland, col. 4, Ins. 18-30). The "secure" environments disclosed by Southerland are not designed to prevent electromagnetic radiation from leaking out, or being eavesdropped on, but rather to detect intrusions into the "secure" environment. (Southerland, col. 7, ln. 58- col. 8, ln. 5) Southerland does not disclose first and second devices, which communicate with each other in a sealed enclosure, rather Southerland discloses a single device (volatile data storage device 301), which is erased when a detector (detector 303) detects an intrusion into the "secure" environment.

Varadharajan discloses the exchange of a security key between a portable device and a host device, locally via a direct link and then subsequently using the key to control or encrypt remote communications. (Varadharajan, col. 4, Ins. 1-13). However, there is no disclosure or suggestion in Varadharajan, that the portable device and the host device should be both placed in the same sealed enclosure, for the key exchange.

Applying Southerland to Varadharajan does not result in the invention of claim 1. A person skilled in the art would, at best, use Southerland to protect an individual device, such as a RAM (random access memory) from tampering, by causing the RAM to be erased upon intrusion.

However, it is not suggested in any way that Southerland should be applied to communications or communications of keys. Furthermore, the "secure" environments of Southerland would not protect the communications of keys, since these environments are not disclosed as preventing electromagnetic leakage.

Claim 1 is submitted to be allowable for at least the foregoing reasons. Claims 2-3 are dependent on claim 1 and are also submitted to be allowable for at least the same reasons.

Claim 14 specifies:

14. A method comprised of the steps of:
placing a first device into an enclosure;
connecting the first device to a transmitter, wherein the transmitter is connected to a first end of a cord device the first end of the cord device being inside the enclosure;
sealing the enclosure while the first device is in the enclosure and while the first device is connected to the transmitter;
wherein the cord device has a second end which is outside the enclosure; and
wherein
the method further is comprised of connecting a second device, which lies outside the enclosure, to the second end of the cord device;
and after connecting the first device to the first end of the cord device and after connecting the second device to the second end of the cord device, causing the first device to exchange a key with the second device while the first device is in the sealed enclosure;
removing the first device from the enclosure after the key exchange; and
using the key to allow the first device and the second device to communicate with each other using methods of encryption with the first device outside of the enclosure.

In the present application, in one or more embodiments, a first device 570 is placed into an enclosure including container 500 and cover 508. (Present application, Fig. 9, pg. 12, last paragraph – pg. 13, first paragraph). The first device 570 is connected to a transmitter 538. The transmitter 538 is connected to the first end of a cord device (540), the first end of the cord device being in the enclosure (container 500 and cover 508). The enclosure (500 and 508) is sealed while the first device 570 is in the enclosure and while the first device 570 is connected to the transmitter 538. The cord device has a second end 544, which is outside the enclosure (500, 508), to which a second device 580 is connected. A key is exchanged between first device 570

and second device 580 while the first device 570 is in the sealed enclosure. The first device 570 is removed from the enclosure after the key exchange and subsequently the key is used to allow the first and second devices to communicate with each other outside of the enclosure (500, 508).

As previously discussed, Southerland deals with erasure of data in a storage device and does not deal with communication of keys. Also as previously discussed, Varadharajan does not in any way disclose providing sealed enclosures for key exchanges between first and second devices, such as for preventing electromagnetic radiation leakage, or eavesdropping.

Claim 14 is submitted to be allowable for at least the foregoing reasons. Claims 15-17 are dependent on claim 14 and are submitted to be allowable for at least the same reasons.

Claim 19 specifies:

19. An apparatus comprising:
means for causing a first device to exchange a key with a second device; and
means for preventing a third device from determining a key which is exchanged between the first device and the second device, and
wherein the means for preventing the third device from determining the key is comprised of an enclosure having a filtering material;
wherein the enclosure is adapted to that it can completely surround both the first device and the second device in order to prevent the third device from determining the key.

As previously discussed, Southerland deals with erasure of data in a storage device and does not deal with communication of keys. Also as previously discussed, Varadharajan does not in any way disclose providing sealed enclosures for key exchanges between first and second devices, such as for preventing electromagnetic radiation leakage, or eavesdropping. In addition, neither Southerland nor Varadharajan disclose an enclosure including filtering material.

Claim 19 is submitted to be allowable for at least the foregoing reasons. Claims 20-21 are dependent on claim 19 and are submitted to be allowable for at least the same reasons.

Claim 25 specifies:

25. A method comprising:
placing a first device in an enclosure;
placing a second device in the enclosure;

sealing the enclosure while the first device and the second device are in the enclosure;
causing the first device to exchange a key with the second device while the first device and the second device are in the enclosure and while the enclosure is sealed;
removing the first device and the second device from the enclosure after the key exchange; and
using the key to allow the first device and the second device to communicate with each other using methods of authentication outside the enclosure.

As previously discussed, Southerland deals with erasure of data in a storage device and does not deal with communication of keys. Also as previously discussed, Varadharajan does not in any way disclose providing sealed enclosures for key exchanges between first and second devices, such as for preventing electromagnetic radiation leakage, or eavesdropping.

Claim 25 is submitted to be allowable for at least the foregoing reasons.

The examiner makes many statements, which the applicant disagrees with. The applicant will only address some of these statements but may also disagree with other statements.

The examiner states that:

"... Varadharajan discloses ... removing the first device and the second device from the enclosure after key exchange; ... (4/6/2005, Office action, pg. 4, paragraph 1).

The above statement is incorrect. Varadharajan does not place first and second devices into an enclosure and Varadharajan does not remove first and second devices from an enclosure after a key exchange. The examiner does not identify the purported enclosure, because there is no such enclosure in Varadharajan.

The examiner states that:

"... Southerland provides details of secure and sealed enclosure to interconnect two devices. Southerland could have been modified by Varadharajan to arrive at the claimed invention by having the first and second devices in the secure enclosure and logically exchanging a key to communicate with each other outside the secure environment." (4/6/2005 office action, pg. 4, paragraph 5).

The applicant disagrees. Firstly, Southerland is directed towards erasing the data of a single volatile data storage device when an intrusion into an environment is detected.

(Southerland, col. 4, Ins. 18-30). Southerland's "secure" environments, such as a spatial region defined by a magnetic field or optical beams, or merely providing a mechanically sealed housing (without the proper material) (Southerland, col. 7, Ins. 57-67), will not prevent eavesdropping on communications or leakage of electromagnetic radiation providing information about communication of a key.

In addition, whether Southerland "could have been modified by Varadharajan" to arrive at the claimed invention is not the proper question. The question is whether there is any suggestion and there is none. Southerland erases data storage devices in response to intrusions and does not suggest or disclose protecting communications.

The examiner states that:

"Varadharajan discloses ... causing the first device to exchange a key with the second device while the first device is in the sealed enclosure; removing the first device from the enclosure after the key exchange; and using the key to allow the first device and the second device to communicate with each other using methods of encryption with the first device outside of the enclosure." (4/6/2005 office action, pg. 5, last paragraph – pg. 6, first paragraph).

The examiner is incorrect. Varadharajan does not disclose a first device in a sealed enclosure for a key exchange and then removing the first device from the enclosure for later communication. The examiner does not identify such an enclosure in Varadharajan, because there is no such enclosure.

The examiner states that:

"Southerland could have been modified by Varadharajan to arrive at the claimed invention by having the first and second devices in the secure enclosure and logically exchanging a key to communicate with each other outside the secure environment." (4/6/2005, office action, pg. 6, paragraph 7).

The examiner is incorrect. Southerland does not protect communications but rather destroys data in response to intrusions. Exchanging a key in Southerland's "secure" environment, would not protect the communications from leaking out to eavesdroppers, for example in the form

of electromagnetic radiation leakage. In addition the question shouldn't be what "could have been modified" but rather whether there is a suggestion to do so, and there is no suggestion.

The examiner states that:

"Southerland discloses means for causing a first device to exchange a key ... with a second device ... means for preventing a third device from determining a key ... wherein the means for preventing a third device from determining the key is comprised of an enclosure having a filtering material ... wherein the enclosure is adapted ... in order to prevent the third device from determining the key...." (4/6/2005 office action, pg. 6, paragraph 8 – p. 7, paragraph 8).

The examiner is incorrect. Southerland has absolutely nothing to do with the exchange of a key. Southerland erases data of a data storage device in response to an intrusion.

III. Rejection of claims 4-13 under 35 U.S.C. 103(a) based on Southerland in view of Varadharajan and further in view of Reidinger et al.

The examiner has rejected claims 4-13 under 35 U.S.C. 103(a) based on Southerland in view of Varadharajan and further in view of Reidinger et. al.

Claims 4-13 are dependent on claim 1 which specifies:

1. A method comprising:
placing a first device in an enclosure;
placing a second device in the enclosure;
sealing the enclosure while the first device and the second device are in the enclosure;
causing the first device to exchange a key with the second device while the first device and the second device are in the enclosure and while the enclosure is sealed;
removing the first device and the second device from the enclosure after the key exchange; and
using the key to allow the first device and the second device to communicate with each other using methods of encryption outside the enclosure.

As previously discussed, Southerland deals with erasure of data in a single data storage device and does not deal with communication of keys. Also as previously discussed, Varadharajan does not in any way disclose providing sealed enclosures for key exchanges

between first and second devices, such as for preventing electromagnetic radiation leakage, or eavesdropping. Reidinger provides an antimagnetic plastic bag 3b in which a single circuit board 4b is enclosed (Reidinger, col. 3, Ins. 9-15) and an antimagnetic plastic bag 3a in which a single circuit board 4a is enclosed (Reidinger, col. 2, ln. 68 – col. 3, ln. 5). Reidinger does not in any way suggest providing sealed enclosures for key exchanges between first and second devices, such as for preventing electromagnetic radiation leakage, or eavesdropping. Claims 4-13 are submitted to be allowable for at least the foregoing reasons.

The examiner states that:

"Southerland and Varadharajan disclose first and second device transmit and receive information to and from each other in a sealed enclosure" (4/6/2005, office action, pg. 9, paragraph 18; pg. 11, paragraph 20; pg. 12, paragraph 22)

The examiner is incorrect. Southerland does not deal with transmission and reception of information in a sealed enclosure. Southerland deals with erasure of data in a storage device when an intrusion is detected. (Southerland, col. 4, Ins. 18-30). Varadharajan does not disclose transmission and reception of information by first and second devices in a sealed enclosure. The examiner does not identify such a sealed enclosure in Varadharajan because there is no such sealed enclosure.

The examiner indicates that Reidinger discloses glass as claimed in claim 8 of the present application. (4/6/2005 office action, pg. 14, paragraph 26). The examiner is incorrect.

IV. Rejection of claims 18, 22, and 24 under 35 U.S.C. 103(a) based on Varadharajan in view of Lemilainen

Claims 18, 22, and 24 have been rejected under 35 U.S.C. 103(a) based on Varadharajan in view of Lemilainen.

Claim 18 is dependent on claim 14 which specifies:

14. A method comprised of the steps of:

16

placing a first device into an enclosure;
connecting the first device to a transmitter, wherein the transmitter is connected to a first end of a cord device the first end of the cord device being inside the enclosure;
sealing the enclosure while the first device is in the enclosure and while the first device is connected to the transmitter;
wherein the cord device has a second end which is outside the enclosure; and wherein the method further is comprised of connecting a second device which lies outside the enclosure, to the second end of the cord device;
and after connecting the first device to the first end of the cord device and after connecting the second device to the second end of the cord device, causing the first device to exchange a key with the second device while the first device is in the sealed enclosure;
removing the first device from the enclosure after the key exchange; and
using the key to allow the first device and the second device to communicate with each other using methods of encryption with the first device outside of the enclosure.

Neither Varadharajan nor Lemilainen, disclose providing a sealed enclosure for a key exchange between a first device and a second device, wherein the first device is in the sealed enclosure and connected to a transmitter which is connected to a first end of a cord device which is inside the enclosure. Claim 18 is submitted to be allowable for at least the foregoing reasons.

Claim 22 specifies:

22. A portable device comprised of:

- a Bluetooth transmitter;
- a port for physically and electronically connecting the portable device to a first device;

wherein in a first mode the Bluetooth transmitter of the portable device locates a second device and performs a key exchange with the second device via a wireless channel;

and wherein in a second mode the port of the portable device is physically and electronically connected to the first device so that the portable device can communicate with the first device; and wherein the portable device communicates a key to the first device obtained from the key exchange with the second device.

In the present application, in one or more embodiments, a portable device 720 is comprised of a Bluetooth transmitter and a port or leads 742 and 744. (Present application, Fig. 11A, 11B). The portable device 720 can be physically and electronically connected to a first device 730 through cable 740. (Present application, Fig. 11B) In a first mode, the blue tooth transmitter of device 720 locates a second device 722 and performs a key exchange with

the second device 722 via a wireless channel. (Present application, Fig. 11A, pg. 14, paragraph 1). In a second mode, the port (leads 742 and 744) of the portable device 720 is physically and electronically connected to the first device 730 so that the portable device 720 can communicate with the first device 730 and wherein the portable device 720 communicates a key to the first device 730 obtained from the key exchange with the second device 722.

Neither Varadharajan nor Lemilainen, disclose a first mode wherein a blue tooth transmitter of a portable device locates a second device and performs a key exchange with the second device.

Claim 22 is submitted to be allowable for at least the foregoing reasons. Claim 24 is dependent on claim 22 and is submitted to be allowable for at least the same reasons as claim 22.

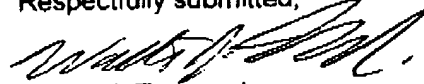
V. New Claims 26-32

The applicant has added new claims 26-32. These claims are dependent on previous claims and are submitted to be allowable for at least that reason. These added claims also include further limitations which, at least in combination with other limitations, are not shown by the prior art cited.

VI. Conclusion

Claims 1-32 are respectfully submitted to be allowable. Favorable reconsideration of this application, as amended, is respectfully requested. A credit card payment form for \$350.00 for extra claims fees is enclosed. (7 additional claims over twenty x \$50.00 = \$350.00).

Respectfully submitted,



Walter J. Tencza Jr.
Reg. No. 35,708
Suite 3
10 Station Place
Metuchen, N.J. 08840
(732) 549-3007
Fax (732) 549-8486